AIR WAR COLLEGE

AIR UNIVERSITY

FOCUS TARGETING IN A COIN ENVIRONMENT

by

Larry D. Perino, LTC, U.S. ARMY

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Page

Chapter 1 - INTRODUCTION

As the United States finds itself in the 10th year of conflict in Afghanistan, it was not until the fall of 2009 that counterinsurgency became the centerpiece of US strategy. Whether they realized it or not, the coalition was fighting an insurgency ever since they pushed the Taliban back into Pakistan in 2003, well before the violence in Iraq and the introduction of the Army and U.S. Marine Corps Counterinsurgency Field Manual. Prior to the adoption of this new strategy, ground forces at all levels made many mistakes. First and foremost among these mistakes was how to see and understand the environment and how to target the enemy. The second mistake (and probably the most important) was that coalition forces became too focused on the enemy. In a counterinsurgency, the focus at all levels from strategic to tactical should be on the entire population and how it interacts with the insurgent. At the operational and tactical level, this understanding of the social network, coupled with a dynamic targeting process, will eventually lead toward success. Unfortunately, the tendency to be purely enemy focused is common at the tactical, operational, and strategic levels and was identified in the article titled "Fixing Intel" by the chief intelligence officer for Afghanistan, MG Flynn, who stated: "because the United States has focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, our intelligence apparatus still finds itself unable to answer fundamental questions about the environment in which we operate and the people we are trying to protect and persuade." [1]

Many senior leaders, especially in the intelligence community, are talking about the need for broad sweeping changes regarding how they should approach the counterinsurgency problem in Afghanistan. In the era of today's extremely complex counterinsurgency (COIN) environment, the changes described by senior leaders and counterinsurgency experts are needed. However, this guidance does not sufficiently describe how to implement these changes at the operational level. Successful units understand that the most effective method of implementing a successful counterinsurgency strategy is through understanding enemy and friendly networks. Understanding these networks and how they interact allows for effective targeting and increased capacity to positively shape the environment.

The Army's counterinsurgency doctrine provides guidance on how to defeat an insurgency. This guidance, however, is considerably different than the traditional doctrine on how the Army has trained and prepared to fight over the past twenty years. Today, many senior military and political leaders recognize that the character of conflict in the 21th Century will be waged among both state and non-state actors. Because of globalization and the technological dominance of the United States military, the United States is more likely to face hybrid threats, consisting of diverse and dynamic combinations of conventional, irregular, terrorist, and criminal capabilities employed asymmetrically to counter military advantages.[2]

To correctly approach these problems, leaders at all levels need to understand that a counterinsurgency, at its base, is a political problem and that the focus should primarily be on the population or environment where that insurgency exists, not just the leadership. In this document, I will first describe how to defeat insurgencies at the strategic level utilizing the current doctrine followed by the United States Army and the U.S. Marine Corps. I will then describe how to use a network modeling approach toward defeating a counterinsurgency at the operational and tactical level. Finally, I will provide some guidance on how to use this network modeling approach to effectively target the insurgency.

Chapter 2 – Counterinsurgency Doctrine

To effectively target in a COIN environment, it is extremely important to understand essentially what an insurgency is and how to counter it at the strategic level. As early as 2004, the United States found itself involved in two insurgencies, one in Afghanistan and one in Iraq. The U.S. quickly realized that despite every intention of getting in and out of both wars quickly and avoid the task of nation-building, that was not going to be the case. The reality is that these two conflicts would require a new way of fighting and current military doctrine needed to change as well.   Unfortunately, the U.S. military did not have a counterinsurgency doctrine to counter these new challenges.

Insurgent warfare is not a new form of conflict. The United States is no stranger to this form of conflict in its history. To be sure, insurgencies have existed as a form of warfare for centuries. Unfortunately, each time the United States has had to relearn the principles of counterinsurgency strategy by trial and error. The U.S. military has attempted several times to address counterinsurgency warfare in publications such as the U.S. Marine Corps' *Small Wars Manual*, published in 1940, and reissued in 1990. In the *Small Wars Manual*, insurgent wars involved conflicts between the regular armies against irregular, or comparatively speaking irregular forces.[3]

However, it wasn't until late in 2006 that the Army, partnered with the United States Marine Corps, institutionalized the concepts and principles of counterinsurgency warfare and published this new doctrine in FM 3-24/MCWP 3-33.5.[*] The intended purpose of FM 3-24 was to provide a baseline for understanding counterinsurgency doctrine, but as a starting point for learning how to conduct complex COIN operations.

To understand COIN, one must first understand what an *insurgency* is and be able to describe its most common characteristics. In Joint Publication (JP 1-02) an insurgency is defined as "an organized movement aimed at the overthrow of a constituted government through the use

[*] For the purposes of brevity, I will refer to FM 3-24/MCWP 3-33.5 as "FM 3-24" for the remainder of the document.

of subversion or armed conflict. It is a politically and military based organization focused on weakening and controlling a centralized government or occupied force."[4] Insurgencies can take many different forms. Additionally, the causes of each insurgency are unique. However, insurgencies do share common attributes and involve four principle actors:

- Insurgents – those hoping to overthrow the established national government or secede from it
- Local government – the central government's security forces as well as key national and local political institutions.
- Outside actors – external states and other non-state entities, who could support either side (central government or insurgency)
- Local population – the most important group of the four. It is the hearts and minds of this group that the central government and the insurgent's fight for. [5]

Counterinsurgency, the antithesis of insurgency, by definition is "military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency."[6] While an insurgency aims to destabilize a central government and increase its control over the population, COIN aims to achieve its goals through the support or buildup of the central government of a country while simultaneously protecting the population from the insurgency.

Counterinsurgency operations require military forces to conduct action across the full spectrum of operations (offensive, defensive, and stability operations) to succeed. These types of operations are tailored based on the situation or mission. Regardless, current COIN doctrine calls for forces to be ready both to fight and to build—depending on the security situation and a variety of other factors. Ultimately, a successful COIN campaign requires more than military actions to ensure success. In fact, a successful COIN operation requires the synchronized application of military, paramilitary, political, economic, psychological, and civic actions.[7]

According to the U.S. COIN doctrine, there are five overarching requirements to achieve success. The first is forces (both Host Nation and U.S.) attacking the insurgent's strategy and bolster/restore the central government's legitimacy. Second is establishing control of areas to operate from and secure the population in those areas. Third is ensuring that the host nation retain or regain control of the major population centers and maintain legitimacy. Forth is expanding operations to regain control of insurgent areas. Finally, is conducting an aggressive information operations (IO) campaign to favorably influence perceptions of the host nation and discredit the insurgents.[8]

The primary approach in conducting a counterinsurgency outlined in FM 3-24 is called the "clear-hold-build" approach. This approach is what was employed in Iraq in 2007 along with the "surge" and is currently the approach used by the United States and its allies today in Afghanistan. In the Clear-Hold-Build approach, the first objective is to create a secure physical and psychological environment. The second objective is to establish firm governmental control of the populace and the area. The third and final objective is to gain the support of the populace.

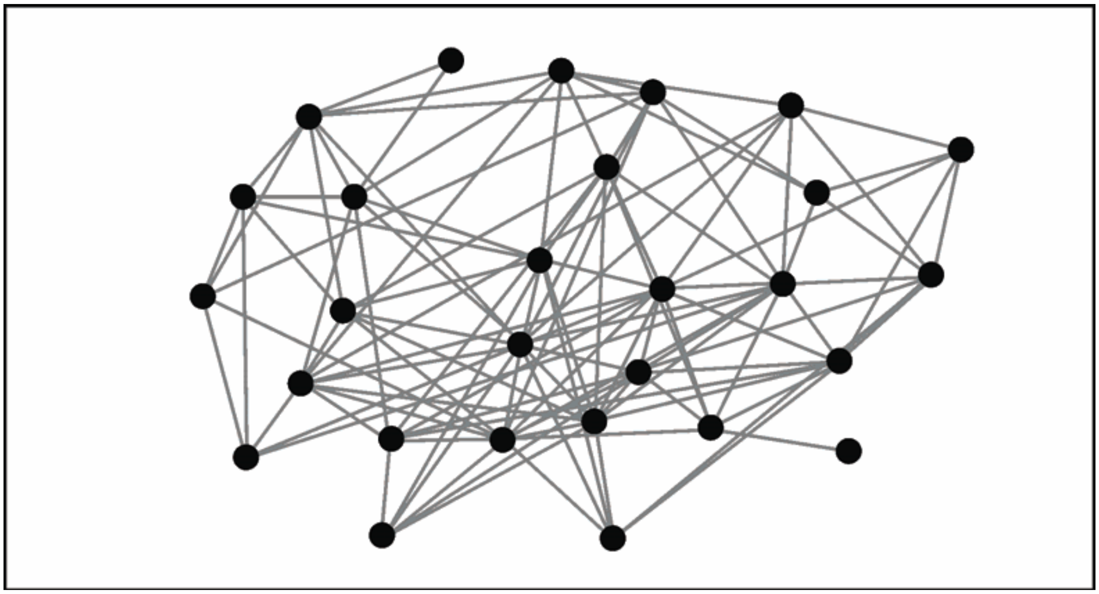
At the strategic level, the clear-hold-build approach is not intended to be a military-only solution. All forms of power: diplomatic, information, economic, and military are used to remove the insurgency's ability to influence the population. The ultimate desire is to enable the central government the ability to begin/resume its support of the population.

Chapter 3 Networks and Centers of Gravity

At times, it seems that translating a strategy to operational and tactical outcomes seems difficult. This phenomenon is no different with COIN. How can a BCT compete with an insurgency to win the "hearts and minds" of the population, the true center of gravity? Given the scope of this paper, I will not attempt to fully explain all the intricacies of counterinsurgency at the operational level. Instead, this paper will attempt to explain how to conduct operations in terms of targeting and how to use limited ISR (intelligence, surveillance, and reconnaissance) and operational assets in a COIN environment.

An insurgency, earlier defined as an "organized movement", is extremely difficult to target at an operational and tactical level. An easier and more useful way is to view an insurgency as a network, or "an interconnected system of things or people".[9] The understanding of the "people" and the "things" that make up an insurgency and how they interact is how forces at the operational and tactical level can conduct effective targeting.

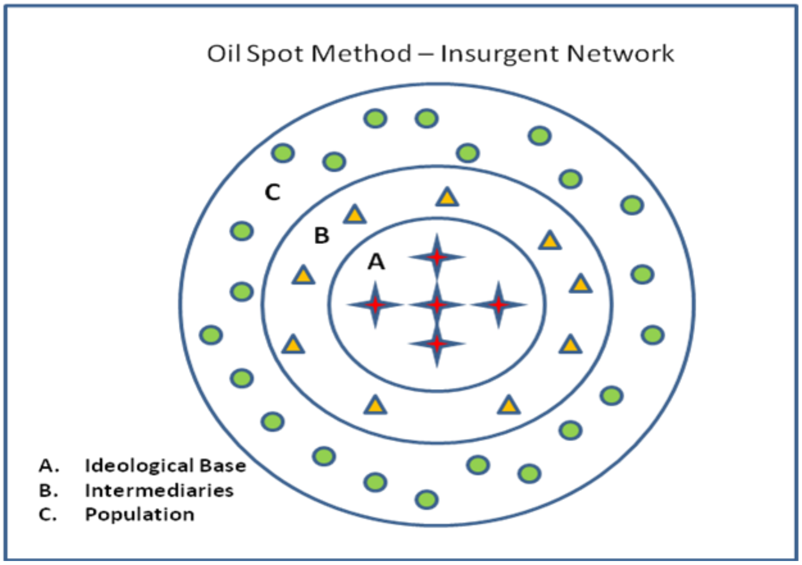
Figure 1- Networked Organization



Looking at an insurgency as a type of social network is a useful way for targeting an insurgent network. Appendix B of FM 3-24, *Counterinsurgency*, provides a description of a social network (Figure 1). Unfortunately, this type of model is extremely complex, and even more difficult to explain without significant study.

An easier and more useful method in describing an insurgent network is by using the Oil Spot Method[†] (Figure 2)[‡]. At the center of the diagram is the core leadership or inner circle of the insurgency. At the second level are the intermediaries and the third level is the population. The core leadership of an insurgency insulates themselves from the population. The core leadership (depicted by the letter "A" in the diagram), does this either because their ideology is unpopular to the population that they want to control or for operational security reasons or risk compromise[10]. To reach the populace, the core leadership uses intermediaries (letter "B") to influence the general population (letter "C"). These intermediaries work on behalf of the leadership to establish links to facilitators and with the population.

Figure 2 - Oil Spot Method

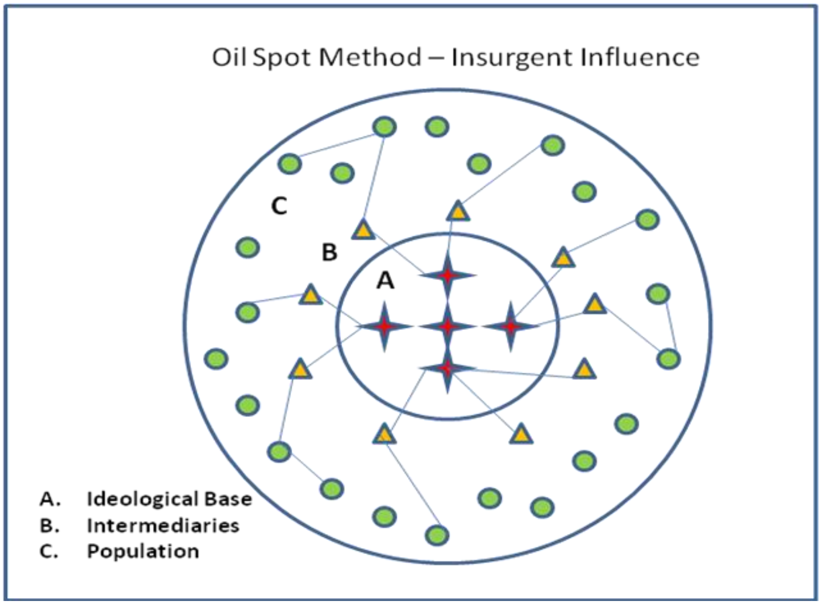


Additionally, intermediaries may share the same ideological beliefs of the insurgent leadership, but can also be motivated by other factors, such as money, revenge, and power.[11]

[†] The Oil Spot method mentioned in this paper differs from the traditional Oil Spot strategy concept advanced by COIN experts David Galula and Andrew Krepenivich.

[‡] Diagram Courtesy of the Asymmetric Warfare Group

Figure 3- Oil Spot Method Insurgent Influence



More importantly, the intermediaries establish connections within their community and also assist in recruiting members for the insurgency (Figure 3)[§].

The Oil Spot Method is a graphic portrayal of an insurgency. However, understanding this is only part of what is required to conduct effective targeting. Another key is to understand "what" to target. This is done by utilizing a center of gravity (COG) analysis as part of the intelligence preparation of the Operational Environment (IPOE). COG analysis translates theory into practice from the bottom up, exposing insurgent lines of operation (LOOs) and suggesting possible counters to them. The ultimate goal in this process is to understand the insurgent's strategy, get inside his decision strategy, and predict his likely actions.[12]

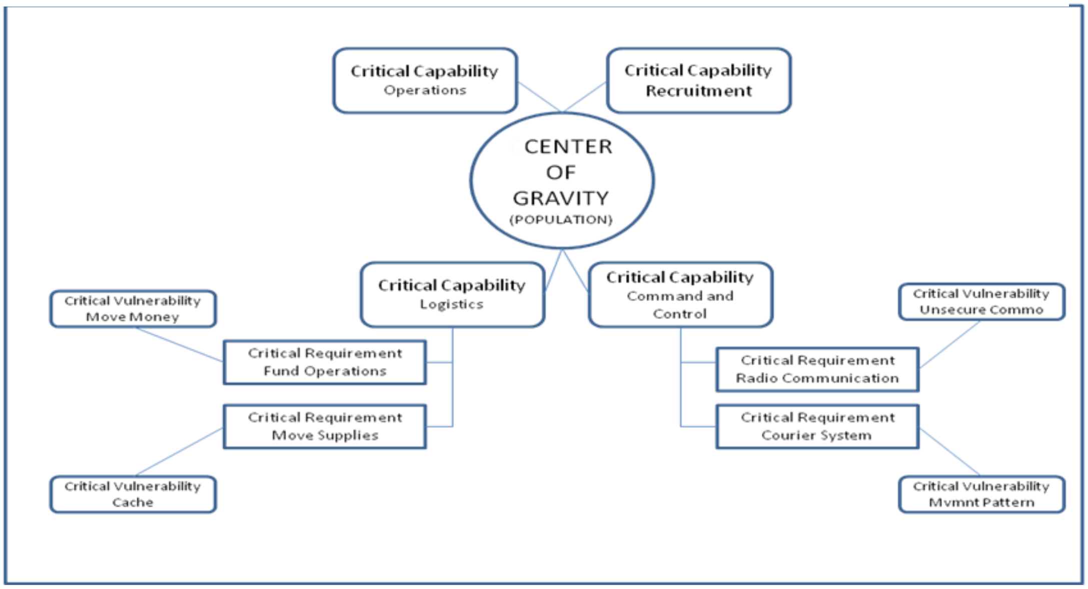
Military theorist Carl Von Clausewitz in his book "On War" defined a center of gravity as: "The hub of all power and movement, on which everything depends." [13] In a COIN environment, the center of gravity is the population. Without being able to control or influence

[§] Diagram Courtesy of the Asymmetric Warfare Group it, an insurgency cannot survive. COGs are a source of power. Critical capabilities are those actions or activities that the center of gravity can do.

In a COG analysis, any center of gravity can have one or multiple critical capabilities, for the purposes of this example, several critical capabilities could be: exercise command and control, recruit, resupply, and conduct operations.

Within each critical capability are required tasks, known at critical requirements. These tasks are essential in the accomplishment of a critical capability. These are actions used (or required) to control or influence the COG. In a COIN environment, critical requirements could range from funding, to transporting supplies and personnel, to IED emplacement. Lastly, several of these requirements are potentially vulnerable to exploitation; in this case, they are called critical vulnerabilities. It is through the exploitation of the enemy's critical vulnerabilities that will enable an organization to focus ISR assets and neutralize the threat. An easy way to remember the difference between a critical capability and a critical requirement/vulnerability is that a critical capability is what a COG "does" and a critical requirement is what a COG "needs".

Figure 4 - Center of Gravity Analysis



Critical Capability Operations
Critical Capability Recruitment
CENTER OF GRAVITY (POPULATION)
Critical Capability Logistics
Critical Capability Command and Control
Critical Vulnerability Move Money
Critical Requirement Fund Operations
Critical Requirement Move Supplies
Critical Vulnerability Cache
Critical Vulnerability Unsecure Commo
Critical Requirement Radio Communication
Critical Requirement Courier System
Critical Vulnerability Mvmnt Pattern

Understanding how a COG analysis works as part of the IPB process is extremely important. It is virtually impossible to immediately attack an enemy's center of gravity, or his critical capability for that matter, in one quick strike or operation, especially at the operational level. A COG analysis will allow a unit to break up the threat in more manageable pieces and is a useful method in identifying the enemy's strengths and weaknesses. Given the limited amount of assets at the operational and tactical levels, focusing on the enemy's weakness provides for a more useful and judicious use of valuable resources.

Chapter 4 Targeting and Social Networks

Centers of gravity analysis and threat network analysis are beneficial toward understanding an enemy's potential weaknesses or vulnerabilities. These may be beneficial in a major theater of war or during combat operations against a standing army. In a COIN, environment, they are not enough. Unfortunately, units at the operational and tactical level become too focused on the enemy and fail to gain a full understanding of the operational environment.

This tendency to fixate on the enemy has not gone unnoticed by senior leaders in the intelligence community. In the January 2010 article, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan", the authors stated: "because the United States has focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, our intelligence apparatus still finds itself unable to answer fundamental questions about the environment in which we operate and the people we are trying to protect and persuade." [14]

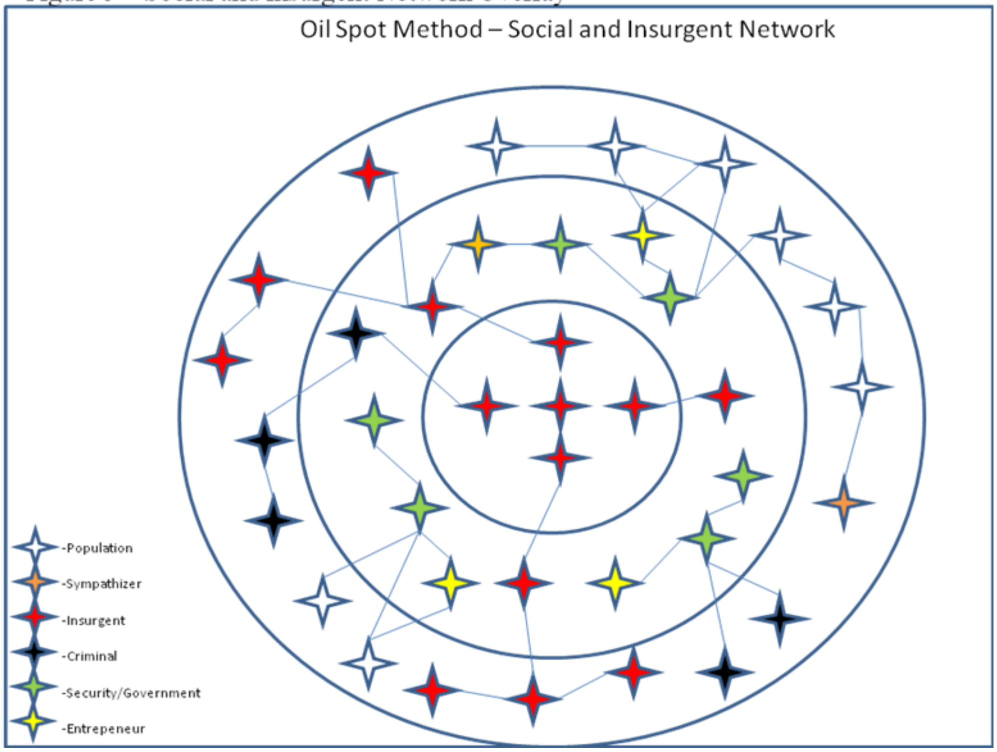
Understandably, it is much harder to find an enemy who lives and operates among the population. It is also extremely difficult to target an enemy without understanding how it interacts with the population. Additionally, by concentrating solely on the enemy, the natural targeting solution would tend to be a kinetic one. Understanding how other social networks interact with a threat network enables units to better comprehend how a threat operates and provides more options towards exploiting a threat's critical vulnerability either kinetically or non-kinetically.

As discussed previously, a threat's center of gravity in a COIN environment is the population and some of its critical requirements include: recruiting, logistics, and command and control. To accomplish these tasks, insurgents need the population to assist them (either willingly or through coercion). Their primary targets are those who most affect the population and are key nodes for various other social networks. These targets could include: land owners, village elders, religious leaders, security forces, local government officials, business owners, and criminal network leaders.[15]

The Army's Asymmetric Warfare Group, a unit whose mission is to provide advisory assistance to U.S. forces in their efforts to counter asymmetric threats, utilizes the oil spot method to describe not only enemy networks, but the interactions between the all networks. In this method, each node is identified by a different color (see Figure 5)[**].

[**] Diagram Courtesy of the Asymmetric Warfare Group

Figure 5 – Social and Insurgent Network Overlay

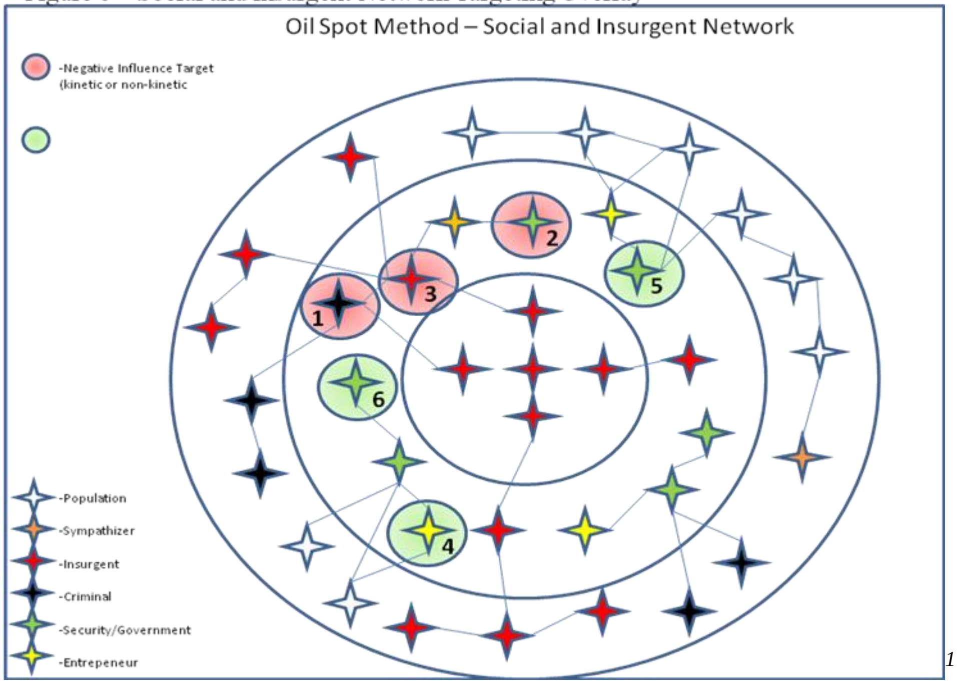


Although this diagram may seem confusing at first, it does give a commander a graphic depiction of how all elements interact with each other. [16] It is the operational and tactical staff's responsibility (not just the S2) to determine how the various factions interact, represented by the solid connecting lines between the different nodes. The merit of this method of depiction is that it shows how an "effect" can be achieved both kinetically AND non-kinetically.

Keep in mind that in this case, the term "targeting" does not necessarily mean to "kill", "capture", or "detain". Instead, the "target" identified could be any key influencer of the population that we would want to support, marginalize, or even kill or capture. The staff at the operational and tactical levels is responsible for providing recommendations on target prioritization and desired effects. This step cannot be overemphasized given limited resources.

The example below (used by the Asymmetric Warfare Group) depicts how targeting is done using this method (See Figure 6).

Figure 6 – Social and Insurgent Network Targeting Overlay


Oil Spot Method – Social and Insurgent Network
-Negative Influence Target (kinetic or non-kinetic
-Population
-Sympathizer
-Insurgent
-Criminal
-Security/Government
-Entrepeneur
1
2
3
4
5
6

[17]

In this example, Target 1 is a drug trafficker who operates in a specific area. Target 2 is a corrupt police official. Target 3 is a local insurgent with direct ties to the insurgent leadership. Target 4 is a business owner and entrepreneur. Target 5 is a local village elder and Target 6 is a security forces battalion commander. Below is a table indicating how a unit might use this targeting method.

Target	Who	What	How	Priority
1	Drug Trafficker	Negative influence	- Capture -Turn over to HN law enforcement	5
2	Corrupt Police Chief	Negative influence	-Warn officer - Prosecute using HN rule of law legal procedures	4
3	Local Insurgent	Negative influence	-Isolate/ Capture/Kill	1
4	Entrepreneur	Positive Influence	-Provide Security/Funds for bazaar construction project	6
5	Village Elder	Positive Influence	-Facilitate meetings with provincial government - vaccinations -funding and security for	2

			irrigation construction project	
6	Security Forces Bn Cdr	Positive Influence	-Conduct joint training/operations -Include in discussions with village elder and local government	3

Understanding that there is not enough information available on the priority target, the local insurgent leader, a unit would move to the next priority, trying to positively influence the village elder. The focus at this stage is eliminating those targets that directly assist the insurgent, the drug trafficker and the corrupt police official with the desired effect of isolating the insurgent and gaining additional intelligence.

Chapter 5 Targeting Processes for COIN

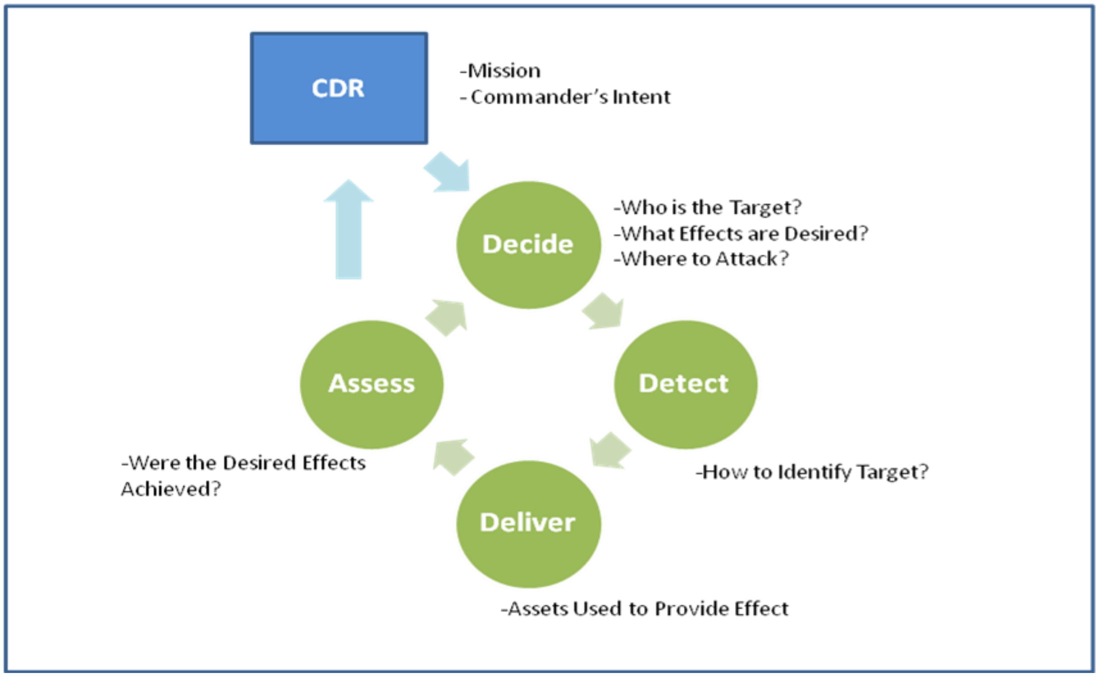
Understanding the nature of the environment and the enemy network within it are the first steps toward successful targeting in the COIN environment. The final step is the actual targeting process. According to joint doctrine, "A target is an entity or object considered for possible engagement or action. It may be an area, complex, installation, force, equipment, capability, function, individual, group, system, entity, or behavior identified for possible action to support the commander's objectives, guidance, and intent."[18]

Targeting involves the selection, prioritization, methods of influence, and desired effects on identified targets. A successful targeting process will define the method of engagement. It should identify whether the effect should be lethal or non-lethal; whether the approach should be direct or indirect; and whether the method of delivery should be kinetic or non-kinetic.

The targeting process in a COIN environment is more difficult compared to targeting in a conventional environment. In a conventional threat, the enemy is easy to find, but could be difficult to kill. Conversely, an insurgent threat is difficult to find, but easy to kill when found.

U.S. Army doctrine utilizes the Decide, Detect, Deliver, and Assess (D3A) as its primary targeting model. The D3A methodology focuses on synchronizing intelligence, maneuver, and fire support to meet the commander's intent. The primary planning process for D3A is the Military Decision Making Process (MDMP). Through this process, the commander defines the organization's mission, priorities, and intent. The commander's guidance provides the impetus for the targeting process (See Figure 7). Through the commander's guidance, an organization identifies and prioritizes the targets, determines the desired effect, and where to attack the target. The Detect phase identifies the asset or assets that will find the target and the Deliver phase determines which asset will provide the desired effect. The final phase, the Assess phase, determines whether the intended effects were met and if the target needs reengagement.

Figure 7 – D3A Targeting Methodology



Overall, the D3A methodology is proven and effective. It is flexible enough for use in both area and personality targeting. However, it is not without its limitations in a COIN environment. While it is effective in translating commander's intent into specific effects, it does not emphasize the need to exploit and analyze information gained for future targeting and the dissemination of that intelligence. Simply put, D3A is more static, extremely useful in deliberate planning situations but difficult to apply when the situation requires immediate re-tasking of assets.

At the joint level, the joint targeting cycle (JTC) is a deliberate iterative targeting process that is not time- constrained and steps may occur concurrently, but provides a framework to describe the steps that must be satisfied to successfully target.[19] The JTC involves several steps: provide CDR guidance, target development, analyze capabilities, commander decision, mission plan/execution, and assess. Although the JTC is slightly different than the D3A method, it still has the same shortcomings that it is more suited for deliberately planned operations and not always favorable for the fluid and dynamic COIN environment.

A more suitable targeting process for the COIN environment is the Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD) method, originally developed for Special Operations Forces (SOF) conducting personality targeting, or "man-hunting". F3EAD is also suitable for conventional forces and is now recognized as doctrine, not as a replacement for D3A, but as a subset of the process.[20]

Figure 8 – F3EAD Targeting Methodology

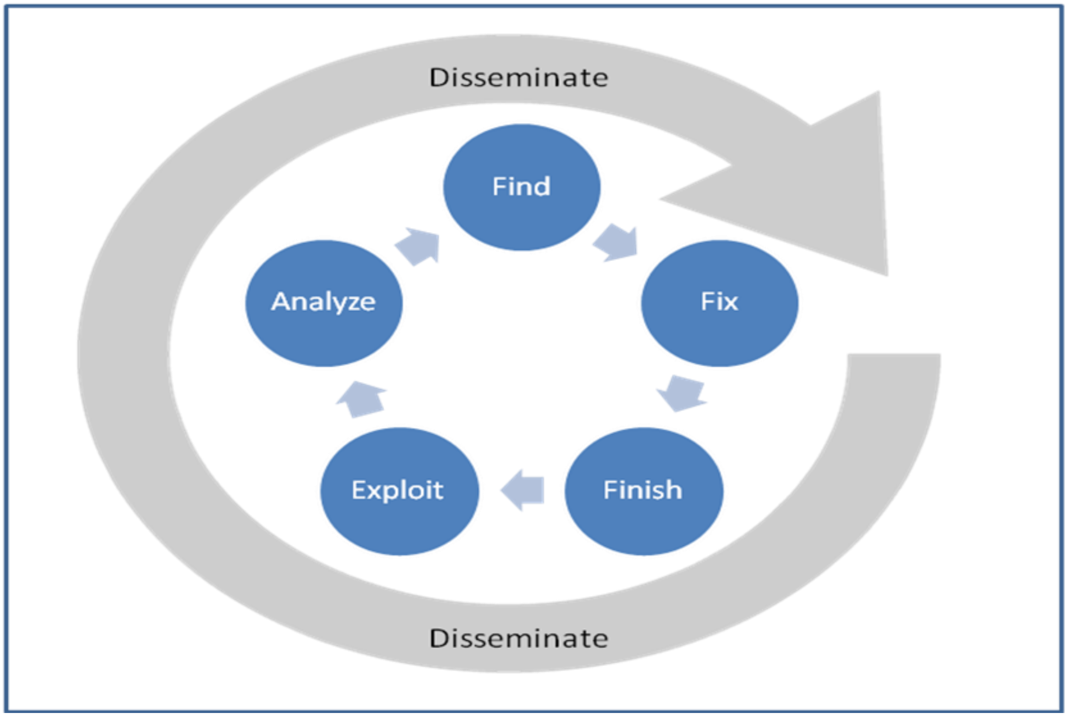


Figure 8 is a graphical description of the F3EAD methodology. F3EAD utilizes the massing of intelligence, surveillance, and reconnaissance (ISR) assets toward locating a specific target. Based on a unit's targeting priorities, the massing of ISR allows for better fidelity in identifying targets hidden among the clutter of non-combatants. It also provides for a better chance of success given the finite number of ISR resources available at the operational level and below. Upon identifying the target, F3EAD emphasizes speed in "fixing" and "finishing" the target. Keep in mind that the term "finishing" can be lethal or non-lethal, kinetic or non-kinetic.

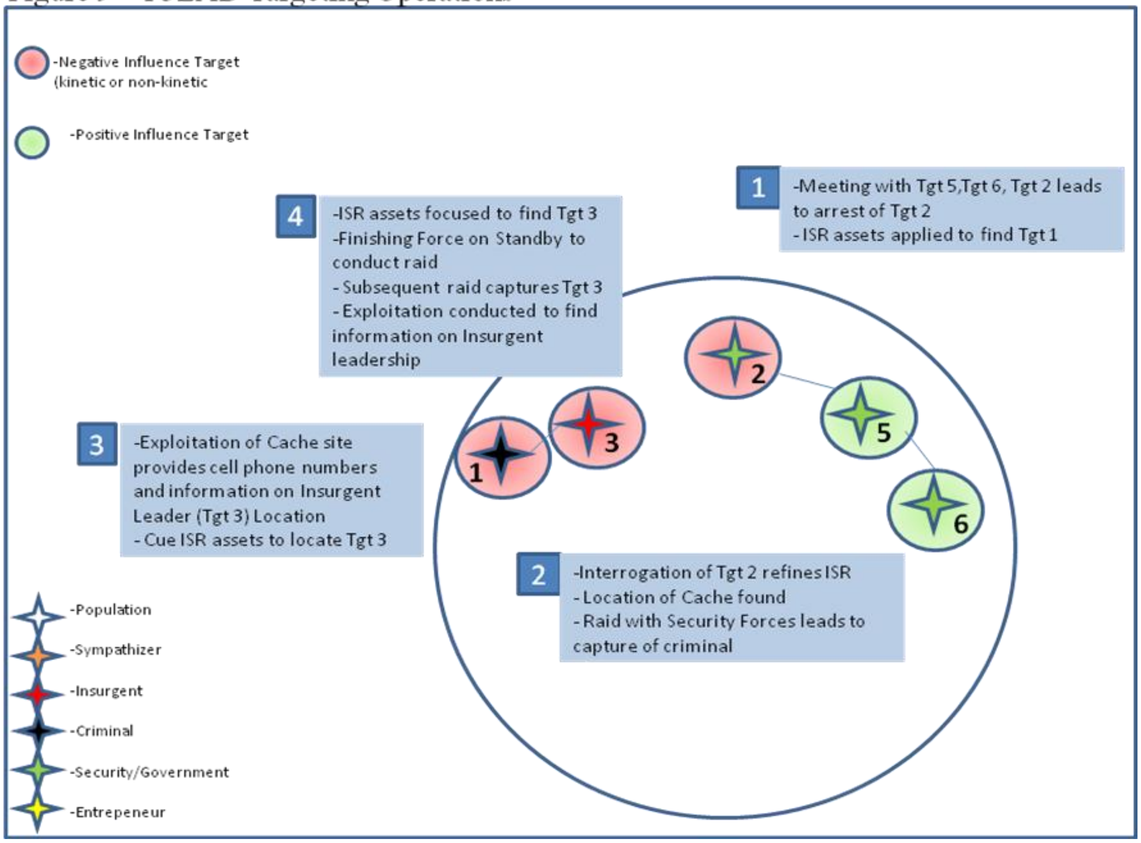
The emphasis on speed in the finish phase enhances the ability to exploit any information found and to analyze it for the development of additional intelligence for future targeting. In many cases, the Exploit and Analyze phases of F3EAD becomes the main effort of the process. Dissemination is continuous throughout the cycle.

F3EAD is useful in attacking an enemy or social network by focusing on the exploit and analyze phases. Information gathered is quickly reinserted into the process and starts the cycle again. The subsequent leads help trace different points within a network for either targeting or assessment. The reliability of intelligence in a COIN environment decreases rapidly over time (people stay in one place for only so long). The rapid turnover of information into intelligence for targeting allows forces to shorten its operational planning cycle. A shortened operational planning cycle ultimately provides a better chance for forces to become “proactive” in their operations vice being “reactive” to enemy actions.

Using the scenario described in the previous section (Figure 6) as an example, a local villager walks in with information on drug smuggling activity. The villager also provides information on how the local insurgency safeguards the movement of drugs by bribing the local police force and intimidation (See Figure 9).

Given this information, the unit decides to concentrate its ISR assets (SIGINT, UAV) along the indicated routes identified by the villager. Simultaneously, the unit gives this information to the local security forces battalion commander (Target 6) and has Target 2 arrested in the presence of the local village elder (Target 5). The result of this action legitimizes the arrest of the police official in the eyes of the elder and creates a positive effect by demonstrating that the security forces were looking out for the best interest of the village.

Figure 9 – F3EAD Targeting Operations



1 -Meeting with Tgt 5,Tgt 6, Tgt 2 leads to arrest of Tgt 2
- ISR assets applied to find Tgt 1

2 -Interrogation of Tgt 2 refines ISR
- Location of Cache found
- Raid with Security Forces leads to capture of criminal

3 -Exploitation of Cache site provides cell phone numbers and information on Insurgent Leader (Tgt 3) Location
- Cue ISR assets to locate Tgt 3

4 -ISR assets focused to find Tgt 3
-Finishing Force on Standby to conduct raid
- Subsequent raid captures Tgt 3
- Exploitation conducted to find information on Insurgent leadership

Interrogation of the police chief provides additional information on drug shipment times and cache sites. A quick reaction force is put on standby and conducts a kinetic raid on a cache site once ISR assets identified a significant increase in activity. Interrogation of the captured drug smuggler (Target 1) and cell phone exploitation provides information on the location of the local insurgent leader (Target 3). Again, the cycle continues as ISR assets are pushed to locate Target 3 until found. Upon locating Target 3, the quick reaction force is again dispatched to conduct a raid to kill or capture the target. This cycle will continue as more information is recovered.

F2EAD is an extremely powerful tool for use in the COIN environment. As you can see from the example provided, it can give a commander extreme flexibility by providing multiple options (using kinetic, non-kinetic, punitive and positive reinforcement methods) in dealing with a very complex problem.

Chapter 6 Conclusion

The United States' military forces are facing what the 2010 Army Posture Statement refers to as "an era of persistent conflict". Challenges will arise across all domains and the Army can expect to conduct operations that span from humanitarian assistance and civil support to counterinsurgency and even general war.[21] A growing trend contributing to the challenges is the emergence of failing or failed states and the ability for violent non-state actors to thrive in them. This trend leads the Army's senior leadership to believe that conflict is likely for decades to come. It is this very challenge which U.S. forces in Afghanistan find themselves in today.

Unfortunately, the U.S. military was initially slow in adopting a counterinsurgency doctrine to address the true nature of its problems. During the introduction and employment of that new doctrine, it became apparent that our intelligence apparatus, especially at the operational and tactical level, was too "enemy" focused instead of concentrating on the environment.

This shift in focus will enable forces to understand how the insurgency operates, where it operates, and where it draws its strength compared to being reactive in nature (waiting for the enemy to do something in order to counter it). Understanding how the social network that surrounds the enemy network provides operational commanders with more options for isolating the enemy from the friendly population other than kinetic solutions. Additionally, focus on the environment helps provide answers sought by higher level commanders.

Understanding the environment and the concept of social networks are the first piece toward successful targeting in a COIN environment. In such an environment, the enemy blends in with the population, is difficult to find, and the only way to identify the insurgent from the population is through understanding the connections between them. Understanding the social network allows a commander to visualize **where** to strike, **who** they are going to affect, and **how** to strike the target (e.g. kinetic/non-kinetic, lethal, non-lethal).

Because the focus of social networks is personality based, using an appropriate dynamic targeting process is extremely essential, especially in an environment where resources are limited and the reliability of intelligence is time-dependant. Personality-based targeting models like the F3EAD model, currently being used by both special operations and conventional forces in Afghanistan, are extremely useful tools for operational and tactical organizations choosing to use the social network model. Regardless of the targeting process used, units must realize that in a COIN environment, all operational and staff functions are involved in developing intelligence and participating in the targeting process, especially when the validity of the intelligence is fleeting and time is of the essence.

Bibliography

Asymmetric Warfare Group. (2009, March). Attack the Network Concepts Part I: Oil-Spot Methodology. Fort George Meade, MD, United States: Asymmetric Warfare Group.

Asymmetric Warfare Group. (2009, March). Attack the Network Concepts Part II: Critical Vulnerabilities and Targeting. Fort George Meade, MD, United States: Asymmetric Warfare Group.

Asymmetric Warfare Group. (2009, April). Attack the Network Concepts Part III: Network Modeling and ISR Synchronization. Fort George Meade, MD, United States: Asymmetric Warfare Group.

Asymmetric Warfare Group. (2010, July). Attack the Network Methodology Part IV: Focused Targeting. Fort George Meade, MD, United States: Asymmetric Warfare Group.

Asymmetric Warfare Group. (2008 , May). Company Intelligence Support Team (CoIST). *AWG Tactical Reference Guide* . Fort George Meade, MD, United States : Asymmetric Warfare Group.

Asymmetric Warfare Group. (2010, April). Integrating Information Operations With F3EAD Targeting. *AWG Tactical Reference Guide* . Fort George Meade, MD, United States: Asymmetric Warfare Group.

Clausewitz, C., edited by Howard, M., & Paret, P. (1984). *On War.* Princeton, NJ: Princeton Press.

Department of Defense. (2001, December 4). *JP 1-02 Department of Defense Dictionary of Military and Associated Terms.* Retrieved September 18, 2010, from DOD Dictionary of Military Terms Web site: http://www.dtic.mil/doctrine/jel/doddict/

Department of Defense. (2007). JP 3-60 Joint Targeting. Washington D.C.

Flynn, M. T., Pottinger, M., & Batchelor, P. D. (2010). *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan.* Washington D.C.: Center for a New American Security.

French, D., & Silvers, J. (2008). *Tactical Trip Report: Fusion Cells.* Fort Meade, MD: Asymmetric Warfare Group.

Godfry, A. (2010). *Insurgent Quotes*. Retrieved 09 16, 2010, from Quote Sea: The Life in Few Words: http://www.quotesea.com/quotes/keywords/insurgent

Headquarters Department of the Army. (2006). *FM 2-22.3 Human Intelligence Collector Operations.* Washington D.C.: Headquarters, Department of the Army.

Headquarters, Department of the Army and Headquarters, Department of the Marine Corps Combat Development Command. (2006). *FM 3-24: Counterinsurgency.* Washington D.C.: Headquarters, Department of the Army.

Headquarters, Department of the Army. (2009). *FM 3-24.2: Tactics in Counterinsurgency.* Washington D.C.: Headquarters, Department of the Army.

Joint Interagency Explosive Device Defeat Organization. (2010, March). Full Spectrum Targeting. Washington D.C., United States: Joint Interagency Explosive Device Defeat Organization (JIEDDO).

Jones, S. G. (2008). *Counterinsurgency in Afghanistan.* Retrieved September 9, 2010, from RAND National Defense Research Institute: http://www.rand.org/pubs/monographs/2008/RAND_MG595.pdf

Kilcullen, D. (2009). *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One.* New York: Oxford University Press.

Mansoor, P. R., & Ulrich, M. S. (2007, September - October). Linking Doctrine to Action: A New COIN Center-of-Gravity Analysis. *Military Review* , pp. 45-51.

McHugh, J. M., & Casey, G. W. (2010). *A Statement on the Posture of the Unted States Army 2010.* Washington D.C.: Headquarters, Department of the Army.

O'Hanlon, M. E., & Sherjan, H. (2010). *Toughing it Out in Afghanistan.* Washington D.C.: Brookings Institution Press.

Petraeus, D. H. (2010, August 1). COMISAF's Counterinsurgency Guidance. Kabul, Afghanistan: International Security Assistance Force/United States Forces-Afghanistan.

Princeton University. (2010, September 20). *WordNet Search -3.0*. Retrieved October 20, 2010, from WordNet Search: http://wordnetweb.princeton.edu/perl/webwn?s=network

Propes, D. N. (2009, March-April). *Targeting 101: Emerging Target Doctrine.* Retrieved October 18, 2010, from sill-www.army.mil: http://sill-www.army.mil/firesbulletin/2009/Mar_Apr_2009/MAR_APR_2009_Pages15_17.pdf

Record, J. (2009). *Beating Goliath: Why Insurgencies Win.* Dulles: Potomac Books, INC.

Sentse, R., & Jansen, J. (2008, Spring). Fusion A Behavioural Approach to Counterinsurgency. *Journal of Military and Strategic Studies* , pp. 1-16.

Tomio, P. (2009, November 27). *Changing the Culture of Military Intelligence.* Retrieved August 14, 2010, from AEI Center for Defense Studies: http://www.defensestudies.org/?p=1153#more-1153

Van Creveld, M. (2007). *Miscellaneous Military Quotes (Unsorted)*. Retrieved 10 20, 2010, from Digital Attic 2.0: http://www.pvv.ntnu.no/~madsb/home/war/misc_quotes.php

Wolfberg, A. (2006, July - August). Full Spectrum Analysis. *Military Review* , pp. 35-42.

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

[1] Flynn, Pottinger, Batchelor, *Fixing Intel, 4.*
[2] McHugh and Casey, *A Statement on the Posture of the United States Army 2010*, 2.
[3] Record, *Beating Goliath: Why Insurgencies Win*, 111.
[4] Department of Defense, *Joint Publication(JP) 1-02, Department of Defense Military and Associated Terms*, 1 December 2001.
[5] Jones, *In the Graveyard of Empires: America's War In Afghanistan*, 152-153.
[6]Department of Defense, *JP 1-02*, 1 December 2001
[7] Headquarters, Department of the Army and Department of the Marine Corps Combat Development Command, *FM 3-24: Counterinsurgency*, PP?
[8] Headquarters, Department of the Army and Department of the Marine Corps Combat Development Command, *FM 3-24: Counterinsurgency*, PP?
[9] Princeton University WordNet Search, 20 September 2010.
[10] Asymmetric Warfare Group, *Attack the Network Concepts Part 1*, 4.
[11] Asymmetric Warfare Group, *Attack the Network Concepts Part 1*, 6.
[12] Mansoor, Ulrich, *Linking Doctrine to Action: A New COIN Center of Gravity Analysis*, 51.
[13]Clausewitz, *On War*, 595-596.
[14] Flynn, Pottinger, Batchelor, *Fixing Intel, 2009, 4.*
[15] Asymmetric Warfare Group, *Attack the Network Concepts Part 4*, 5.
[16]Asymmetric Warfare Group, *Attack the Network Concepts Part 4*, 6.
[17] Asymmetric Warfare Group, *Attack the Network Concepts Part 4*, 8.
[18] Department of Defense, JP 3-60 Joint Targeting, 2007, pp. I-2,
[19] Ibid, I-2.
[20] Propes, David N., Targeting 101: Emerging Targeting Doctrine, 2009
[21] McHugh and Casey, *A Statement on the Posture of the United States Army 2010*, 2.